

Notice of Allowability

Application No.

09/731,836

Examiner

Michael Pyzocha

Applicant(s)

WRENCH, EDWIN H.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

9-13-06

1. ☒ This communication is responsive to ~~90/31/2006~~ 9-13-06.
2. ☒ The allowed claim(s) is/are 1-15 and 20-30.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Art Unit: 2137

DETAILED ACTION

1. The Appeal Brief and supplemental brief filed on 08/02/2006 and 09/13/2006 have been received and considered.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Stuart Shapiro on 11/14/2006.

The application has been amended as follows:

1. (Previously Presented) A system for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said system comprising:

 a security module for said network interface to facilitate retrieval of information from said user in the form of voice signals and to detect a secure web server providing encrypted sessions and identify security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

 a storage unit to store remote from said network interface voice and security information associated with authorized users of said system, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

 a security system to communicate with said security module and said storage unit and to process for said network interface

Art Unit: 2137

said identified security information to enable said secure encrypted session, wherein said security system includes:

a verification module to verify said user as an authorized system user based on a comparison of said user voice signals with said stored voice information;

a retrieval module to retrieve said security information of said verified user from said storage unit; and

a negotiation module to receive said identified security information from said security module and negotiate communication parameters with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

2. (Original) The system of claim 1 wherein said network includes the Internet.

3. (Original) The system of claim 1 wherein said network interface is in communication with a communications device located remotely of said network interface, and said security module facilitates retrieval of said user voice signals from said communications device.

Art Unit: 2137

4. (Original) The system of claim 3 wherein said communications device includes a telephone.

5. (Original) The system of claim 3 wherein said communications device includes a computer system having an audio input device.

6. (Original) The system of claim 5 wherein said audio input device includes a microphone.

7. (Previously Presented) The system of claim 1 wherein said security module includes:

an identification module to identify said security related information received by said network interface from said secure web server;

a communications module to facilitate communications with said security system and said network interface, wherein said communications module includes:

a send module to provide said user information and said identified security information to said security system to facilitate verification of said user and negotiation of said communication parameters;

a receive module to receive a request for said user information, verification results, responses to said identified security information and said negotiated communication parameters from said security system; and

an interface module for providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser; and

a user interface module to facilitate said user information request for retrieval of said user information and to provide said verification results to said user.

8. (Previously Presented) The system of claim 7 wherein said security system further includes:

an identification verification module to validate an identification within said user information associated with an authorized system user;

an access module to retrieve said voice information from said storage unit associated with said identification;

a selection module to select portions of said retrieved voice information and generate said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said

Art Unit: 2137

retrieved voice information, and wherein said verification module verifies said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and said negotiation module processes said identified security information received from said security module and generates said responses thereto with said retrieved security information to negotiate said communication parameters; and

a security communications module to facilitate communications with said security module, wherein said security communications module includes:

a security send module to provide said user information request, said verification results, said generated responses and said negotiated parameters to said security module; and

a security receive module to receive said user voice signals and said identified security information from said security module.

9. (Original) The system of claim 1 wherein said storage unit includes a database.

Art Unit: 2137

10. (Original) The system of claim 2 wherein said stored security information includes private keys and certificates of said authorized system users.

11. (Original) The system of claim 1 further including:
an enrollment module to retrieve voice signals from said authorized system users and process said authorized system user voice signals to produce said voice information for storage in said storage unit.

12. (Previously Presented) A program product apparatus having a computer readable medium with computer program logic recorded thereon for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said program product apparatus comprising:

a security module for said network interface to facilitate retrieval of information from said user in the form of voice signals and to detect a secure web server providing encrypted sessions and identify security related information received by

Art Unit: 2137

said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

a storage module to store remote from said network interface voice and security information associated with authorized users, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers; and

a secure communications module for a security system to communicate with said security module and said storage module and to process for said network interface said identified security information to enable said secure encrypted session, wherein said secure communications module includes:

a verification module to verify said user as an authorized user based on a comparison of said user voice signals with said stored voice information;

a retrieval module to retrieve said security information of said verified user from said storage module; and

a negotiation module to receive said identified security information from said security module and negotiate communication parameters with said secure web server utilizing

Art Unit: 2137

said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

13. (Previously Presented) The program product apparatus of claim 12 wherein said security module includes:

an identification module to identify said security related information received by said network interface from said secure web server;

a communications module to facilitate communications with said secure communications module and said network interface, wherein said communications module includes:

a send module to provide said user information and said identified security information to said secure communications module to facilitate verification of said user and negotiation of said communication parameters;

a receive module to receive a request for said user information, verification results, responses to said identified security information and said negotiated communication parameters from said secure communications module; and

an interface module for providing said responses and said negotiated parameters to said network interface to facilitate

Art Unit: 2137

secure communications over said network between said secure web server and said voice browser; and

a user interface module to facilitate said user information request for retrieval of said user information and to provide said verification results to said user.

14. (Previously Presented) The program product apparatus of claim 13 wherein said secure communications module further includes:

an identification verification module to validate an identification within said user information associated with an authorized user;

an access module to retrieve said voice information from said storage module associated with said identification;

a selection module to select portions of said retrieved voice information and generate said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said retrieved voice information, and wherein said verification module verifies said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said

Art Unit: 2137

identification and said negotiation module processes said identified security information received from said security module and generates said responses thereto with said retrieved security information to negotiate said communication parameters; and

a security communications module to facilitate communications with said security module, wherein said security communications module includes:

a security send module to provide said user information request, said verification results, said generated responses and said negotiated parameters to said security module; and

a security receive module to receive said user voice signals and said identified security information from said security module.

15. (Original) The program product apparatus of claim 12 further including:

an enrollment module to retrieve voice signals from said authorized users and process said authorized user voice signals to produce said voice information for storage in said storage module.

16-19 (Canceled)

20. (Previously Presented) A method of facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites, wherein said network interface includes a voice browser for receiving voice signals from a user and accessing and navigating web sites in accordance with said received voice signals, said method comprising:

(a) retrieving, via a security module, information from said user in the form of voice signals and detecting a secure web server providing encrypted sessions and identifying security related information received by said network interface from said secure web server in response to said voice browser accessing a secure web site of said secure web server based on voice commands from said user, wherein said security related information includes information enabling a secure encrypted session with said secure web server;

(b) storing remote from said network interface voice and security information associated with authorized users in a storage unit, wherein said security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers;

Art Unit: 2137

(c) verifying said user as an authorized user based on a comparison of said user voice signals with said stored voice information via a security system;

(d) retrieving, via said security system, said security information of said verified user from said storage unit; and

(e) receiving said identified security information from said security module at said security system and negotiating communication parameters for said network interface with said secure web server utilizing said retrieved security information to facilitate said secure encrypted session between said secure web server and said voice browser.

21. (Original) The method of claim 20 wherein said network includes the Internet.

22. (Original) The method of claim 20 wherein said network interface is in communication with a communications device located remotely of said network interface, and step (a) further includes:

(a.1) retrieving said user voice signals from said communications device.

23. (Original) The method of claim 22 wherein said communications device includes a telephone.

24. (Original) The method of claim 22 wherein said communications device includes a computer system having an audio input device.

25. (Original) The method of claim 24 wherein said audio input device includes a microphone.

26. (Previously Presented) The method of claim 20 wherein step (a) further includes:

(a.1) providing said user information to said security system to facilitate verification of said user in response to a request from said security system for user information;

(a.2) receiving verification results from said security system and providing said verification results to said user;

(a.3) providing said identified security information to said security system to facilitate negotiation of said communication parameters;

(a.4) receiving responses to said identified security information and said negotiated communication parameters from said security system; and

Art Unit: 2137

(a.5) providing said responses and said negotiated parameters to said network interface to facilitate secure communications over said network between said secure web server and said voice browser.

27. (Previously Presented) The method of claim 26 wherein step (c) further includes:

(c.1) validating an identification within said user information associated with an authorized user;

(c.2) retrieving said voice information from said storage unit associated with said identification;

(c.3) selecting portions of said retrieved voice information and generating said user information request, wherein said generated request includes a request for user information corresponding to said selected portions of said retrieved voice information; and

(c.4) verifying said user by comparing said user voice signals received from said security module in response to said user information request with said stored voice information associated with an authorized user identified by said identification and providing said verification results to said security module; and

step (e) further includes:

Art Unit: 2137

(e.1) processing said identified security information received from said security module and generating said responses thereto with said retrieved security information to negotiate said communication parameters; and

(e.2) providing said responses and negotiated parameters to said security module to facilitate secure communications over said network between said secure web server and said voice browser.

28. (Original) The method of claim 20 wherein said storage unit includes a database.

29. (Original) The method of claim 21 wherein said stored security information includes private keys and certificates of said authorized users.

30. (Previously Presented) The method of claim 20 further including the step of:

(f) retrieving voice signals from said authorized users and processing said authorized user voice signals to produce said voice information for storage in said storage unit.

31-36 (Canceled)

Art Unit: 2137

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance: The detecting of an event as disclosed by Cohen et al. does not correspond to the claimed limitation of detecting a secure web connection within a voice browser. Nor does the prior art teach the negotiation of parameters for secure encrypted sessions in a voice browser based on stored voice and security information. Claims 16-19 have been canceled because they relate to carrier signals, which are not considered statutory under 35 USC 101.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP